Red Check – Documentation

Red Check is a professional detection analysis platform designed for malware developers and security researchers who require accurate and actionable insights into file detection.

It performs deep Windows Defender signature analysis on your malware samples, identifying exactly why and where detections occur. This allows you to precisely modify your files to evade detection efficiently.

By using Red Check, you eliminate guesswork, reduce development costs, and accelerate your time to undetectable binaries.

Powered by Windows Defender

Red Check uses a customized Windows Defender engine that is always updated to the latest version.
Your malware is analyzed directly against Defender's real, current signature database.

There are no simulations or estimations. Detection results are based on actual signature matching performed by a real Defender backend engine.

This guarantees accurate visibility into how your malware would be detected in real-world Windows environments.

Reverse Engineering and Outflanking

Beyond signature detection, Red Check integrates a reverse engineering engine.
Whenever possible, Red Check will automatically reverse engineer and outflank detected payloads, exposing critical information about the original source code behind detections.

This gives you not only raw detection matches but also insights at the code level, allowing you to refine your binaries and neutralize detection signatures more intelligently.

Why Use Red Check?

Immediate Detection Cause Visibility
Identify exactly which parts of your file trigger detection: offsets, regions, section names, and code patterns.

Precise Outflanking and Decompilation
Reverse engineer and extract original code that caused the signature match whenever possible.

Save Development Time and Expenses
No more endless blind patching, rebuilding, and re-encrypting. Surgically adjust your malware based on precise forensic insights.

Accurate, Real-World Data
Detection results are based directly on the real Windows Defender engine and signature sets.

Secure and Private

All uploaded malware files are processed under strict privacy policies.

Files are automatically and permanently deleted from the server one minute after scan finalization.

Neither the uploaded files nor the analysis results are ever submitted to antivirus companies, cloud reputation systems, threat intelligence databases, or telemetry networks.

No cloud submissions. No sharing. Full operational security guaranteed.

How It Works

1. Purchase a License Key
2. Log into the Red Check Portal
3. Upload Your Malware Sample (.exe, .bin, .dll, .docm, .lnk, .ps1)
4. Analyze and Review Detection Causes
5. Optimize Your Malware

Pricing and License Terms

License duration: 8 hours from first login
License cost: $10 USD

Upload and scan unlimited files during your active license window.
No subscriptions. No hidden fees.

Intended Use

Red Check is developed for authorized cybersecurity research, red teaming, penetration testing, and malware development for lawful and educational purposes.

All users must comply with local and international cybersecurity laws.
Unauthorized use for illegal activities is strictly prohibited.

Red Check assumes no responsibility for any misuse, unlawful behavior, or damage caused by users. You use Red Check entirely at your own risk.

Credits

Red Check is developed by Rasta Mouse and MarlboroMan’s Offensive Security and maintained by MarlboroMan's Offensive Security.

Terms of service

By purchasing and using Red Check, you agree to the following Terms of Service.

Authorized Use Only

Red Check is intended solely for lawful cybersecurity research, red teaming, penetration testing, and malware development for educational purposes.

Unauthorized use for illegal, unethical, or malicious activities is strictly prohibited. Users must comply with all applicable local, national, and international laws.

Privacy and Data Handling

Files uploaded to Red Check are automatically deleted one minute after scan finalization.

No files, results, telemetry, or customer data are shared with any third party, antivirus companies, or cloud reputation services.

Limitation of Liability

Red Check and MarlboroMan's Offensive Security assume no responsibility for any misuse, damages, legal consequences, or losses incurred through the use of this platform.

No Refund Policy

All sales are final. Due to the nature of the digital service provided, Red Check does not offer refunds under any circumstances.

Once a license key is issued and access is granted, the sale is considered complete and non-refundable.